



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,919	12/22/2003	David Carroll Challenger	RPS920030244US1	8405
63203	7590	02/26/2009		
ROGITZ & ASSOCIATES 750 B STREET SUITE 3120 SAN DIEGO, CA 92101			EXAMINER YOUNG, NICOLE M	
			ART UNIT	PAPER NUMBER
			2139	
			MAIL DATE	DELIVERY MODE
			02/26/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte DAVID CARROLL CHALLENGER, DARYL CARVIS CROMER,
HOWARD JEFFREY LOCKER, HERNANDO OVIES, and
RANDALL SCOTT SPRINGFIELD

Appeal 2008-3872
Application 10/748,919
Technology Center 2100

Decided:¹ February 26, 2009

Before JOSEPH L. DIXON, HOWARD B. BLANKENSHIP, and
JEAN R. HOMERE, *Administrative Patent Judges*.

BLANKENSHIP, *Administrative Patent Judge*.

DECISION ON APPEAL

¹ The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1-22, which are all the claims in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

Instant Invention and Rejection

Appellants' invention relates to wireless network computers. When an authenticated wireless computer loses connectivity to a wireless access point of a network and roams to another access point, the computer determines whether the new access point is authorized for secure communication and, if so authorized, releases access to secure data on the network through the new access point. (Abstract.)

Claims 1, 7, and 19 are illustrative of the aspects of the invention as they are claimed.

1. A service comprising:
determining that a mobile computer has lost connectivity to a first access point of a network;
when the mobile computer roams to a second access point of the network, determining whether the second access point is authorized for first secure communication and if so,
releasing access of the computer to first secure data on the network through the second access point, and otherwise releasing access of the computer to data other than the first secure data on the network through the second access point.

7. A mobile computer, comprising:
at least one processor;
at least one wireless transceiver in communication with the processor; the processor executing logic including:
determining whether a predetermined communication hardware event has occurred; and
if a predetermined communication hardware event has occurred, selectively configuring the computer in a non-secure mode in which data on a network is accessed by the computer but not all secure data available on the network can be accessed by the computer.
19. A method comprising:
establishing communication between a mobile computer and a network through an access point; and
based on at least one of: a location, or an identification, of the access point, either granting the computer access to secure assets in the network or granting the computer access to other than the secure assets in the network.

The Examiner relies on the following reference as evidence of unpatentability:

Sumner	2003/0142641 A1	Jul. 31, 2003
--------	-----------------	---------------

Claims 1-22 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Sumner.

An earlier rejection of the claims under 35 U.S.C. § 112 has been withdrawn.

Anticipation

Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim. *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1458 (Fed. Cir. 1984).

Sumner

Sumner is directed to management of wireless network data. Sumner Abstract. The reference describes managing data on multiple WLANs (wireless local area networks) having multiple access points with overlapping coverage. *See generally* Sumner Fig. 3; ¶¶ [0026] - [0030].

Grouping of claims

We rely on the Examiner's findings in the Answer in support of the rejection for anticipation. We will consider and discuss separate claims to the extent that Appellants provide separate arguments for patentability in the Appeal Brief. *See* 37 C.F.R. § 41.37(c)(1)(vii).

I. Claim 7

Appellants submit that claim 7 distinguishes over Sumner because it requires determining whether a predetermined hardware event has occurred and, if so, selectively configuring the computer in a non-secure mode in which data on a network is accessed by the computer, but not all secure data available on the network can be accessed by the computer. (App. Br. 4-5.)

The Examiner responds that Sumner paragraph [0063] indicates the wireless connection being lost -- i.e., "WLAN coverage is lost." According to the Examiner, the connection being lost is a "predetermined communication hardware event" as recited in claim 7. In response to this event, the computer enters a doze mode in which it cannot access secure data. "On the drive to the hotel," a notice is sent that new email has been received. This email notice is the data accessed by the computer from the network when in a non-secure mode. (Ans. 9.)

Claim 7 does not limit the "predetermined communication hardware event" to occurring while accessing data on the "network" recited in the final paragraph of the claim. The Examiner's reading of selectively configuring the computer in a non-secure (doze or sleep) mode in which data on a network is accessed (the notice to search for WLAN service) by the computer is reasonable in view of the claim breadth. The further reading of "but not all secure data available on the network can be accessed by the computer" is also reasonable, as Sumner describes only a limited amount of data being accessed while in the doze or sleep mode, and certainly "not all secure data available on the network" can be accessed by the computer while in the doze or sleep mode.

We therefore consider Sumner to provide more than adequate support for the Examiner's findings with respect to claim 7. The law of anticipation does not require that a reference "teach" what an applicant's disclosure teaches. Assuming that a reference is properly "prior art," it is only necessary that the claims "read on" something disclosed in the reference, i.e., all limitations of the claim are found in the reference, or "fully met" by it. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 772 (Fed. Cir. 1983).

II. Claim 19

Claim 19 recites establishing communication between a mobile computer and a network through an access point, and based on at least one of an identification of the access point, either granting the computer access to secure assets in the network or granting the computer access to other than the secure assets in the network. The Examiner finds that both the "location" and "identification" bases of claim 19 are met by Sumner. (Ans. 7.)

Sumner at paragraph [0024] explains that WEP (wired equivalent privacy) information is used in cooperation with an authentication mechanism to assure only authorized device access. The reference at paragraph [0060] describes both WEP and open access with respect to access points, in addition to the option of requiring a user-unique login and password.

We agree with the Examiner that Sumner meets the terms of claim 19, in granting the computer access to secure assets in the network (e.g., requiring WEP and/or a user login and password), or granting the computer

access to other than the secure assets in the network (e.g., an access point that does not require WEP or a login and password). We also note that Sumner at paragraph [0024] discloses that an access point may also possess information to ascertain the authority of users accessing the network, and may exercise control over network assets for users who have greater or lesser authority to access network attributes such as reachable destinations or sources. In that case, granting of access to secure or other than secure assets of the network is based on at least “an identification” of the access point, such as the SSID (Service Set ID) of the access point. *See* Sumner ¶¶ [0056], [0060].

III. Claim 1

For the limitations of claim 1, the Examiner again relies on the scenarios set out in paragraph [0060] of Sumner. (Ans. 3-4, 8-9.)

Claim 1 reads, not inconsistent with the Examiner’s findings, on a mobile computer in the Sumner reference accessing a first and a second access point, where both access points require WEP and/or a user login and password. If the second access point is determined to be authorized for “first” secure communication, claim 1 continues, “if so,” releasing access of the computer to first secure data on the network through the second access point, “and otherwise releasing access of the computer to data other than the first secure data on the network through the second access point.”

The claim that Appellants have brought on appeal does not require the alternative of releasing access to “first secure data” through the second access point as opposed to releasing access to non-secure data through the

second access point. The claim as drafted requires no more than releasing access to some undefined “first secure data,” while at the same time releasing access to data in addition to the “first” secure data that may also be secure data, but different from the “first” secure data.

We thus agree with the Examiner that Sumner anticipates the subject matter of claim 1.

IV. Claims 3, 16, and 21

With respect to dependent claims 3, 16, and 21, we agree with Appellants to the extent that the Examiner has not provided a sufficient basis, in the Specification or in the reference, to conclude that Sumner describes a “hypervisor” as claimed.

We are thus persuaded of error in the rejection of claims 3, 16, and 21.

V. Claims 6, 7, and 19

With respect to claim 6, we agree with Appellants that Sumner has not been shown to anticipate. As made plain in the statement of the rejection (Ans. 5) and the Examiner’s response to Appellants’ arguments (*id.* at 11), the recitations of claim 6 are read on more than one network described in Sumner (e.g., hotel WLAN, company WLAN, field office WLAN). The claim 6 limitations, however, relate to “the” network recited in base claim 1 -- i.e., a single network that has at least two access points.

Although Appellants suggest that claims 6, 9, and 22 should be grouped together, Appellants rely on the limitations of claim 6, while claims 9 and 22 are each of scope different from the argued claim. Claims 9 and 22

have not been argued separately; thus, no error has been shown in the rejection of claim 9 and 22, which depend from base claims 7 and 19, respectively.

We are therefore persuaded of error in the rejection of claim 6, but not in the rejection of claim 9 or 22.

VI. Summary

Appellants have persuaded us of error in the rejection of claims 3, 6, 16, and 21, but of not in the rejection of any other claims on appeal. We thus sustain the § 102 rejection of claims 1, 2, 4, 5, 7-15, 17-20, and 22, but not the rejection of claims 3, 6, 16, and 21.

CONCLUSION

The Examiner's rejection of claims 1-22 under 35 U.S.C. § 102(e) as being anticipated by Sumner is affirmed with respect to claims 1, 2, 4, 5, 7-15, 17-20, and 22, but reversed with respect to claims 3, 6, 16, and 21.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED-IN-PART

msc

ROGITZ & ASSOCIATES
750 B STREET
SUITE 3120
SAN DIEGO CA 92101